Indicator Matrix of Federal Law and Policy That Parallels the ISE Privacy and Civil Liberties Implementation Guide Process

Background:

Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) , as amended, calls for the issuance of guidelines to protect privacy and civil liberties in the development and use of the "information sharing environment" (ISE). Section 1 of Executive Order 13388 ("Further Strengthening the Sharing of Terrorism Information to Protect Americans") provides that, "[t]o the maximum extent consistent with applicable law, agencies shall … give the highest priority to … the interchange of terrorism information among agencies … [and shall] protect the freedom, information privacy, and other legal rights of Americans in the conduct of [such] activities …." Guidelines for the implementation of these requirements were developed at the President's direction by the Attorney General and the Director of National Intelligence, in coordination with the heads of executive departments and agencies (agencies) that possess or use intelligence or terrorism related information in the ISE. The ISE Privacy Guidelines were approved by the President and issued by the Program Manager for the ISE (PM-ISE) on December 4, 2006.

The ISE Privacy Guidelines require agencies to identify applicable privacy laws, regulations, policies, and other authorities to determine whether policies and procedures are in place for all protected information in the ISE, identify gaps, and formulate any policies or procedures required to fill the gaps. Many agencies have already completed the bulk of these activities in the course of complying with cross-cutting federal laws and policies.

To assist agencies with leveraging work already conducted in these areas, the ISE Privacy Guidelines Committee has reviewed five federal authorities with broad applicability to information sharing by federal agencies and identified requirements that are similar or identical to those required by the ISE Privacy Guidelines. These authorities are:

- The Privacy Act of 1974
- The Privacy Management Report, as required under the implementation guidelines for the Federal Information Security Management Act of 2002 (FISMA)
- OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (September 26, 2003)
- OMB Memorandum 06-15, *Safeguarding Personally Identifiable Information* (May 22, 2006)
- OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007)

This Matrix is offered to federal agencies participating in the ISE as an aid to addressing the requirements of the ISE Privacy Guidelines. It is not intended to be comprehensive, and most agencies are subject to additional privacy-related authorities that they may also leverage in order to develop their ISE privacy-protection plan.

Table I. Comparison of ISE Privacy and Civil Liberties Implementation Guide to Cross-Cutting Federal Agency Requirements

STAGE I								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15[1]**	**OMB M-07-16[2]**	**Comment**
1	2 of 6	**Identify** any applicable laws, Executive Orders, policies, and procedures that apply to protected information that the agency will make available or access through the ISE (ISE Privacy Guidelines, Section 2 (a and b)).	X	X	—	X	X	
1	2 of 6	Consider including terrorism related information sharing practices that may be more informal, as well as any proposed terrorism information sharing plans in documentation.	X	—	—	X	—	
1	2 of 6	Identify collection (acquisition and access) laws, Executive Orders, policies, and procedures.	X	—	—	X	X	
1	2 of 6	Identify retention (storage, safeguarding, and validation) laws, Executive Orders, policies, and procedures.	X	—	—	X	—	
1	2 of 6	Identify production (dissemination and publication) laws, Executive Orders, policies, and procedures.	X	—	X	X	X	
1	2 of 6	Identify use (action and response taken upon receipt of such information) laws, Executive Orders, policies, and procedures.	X	—	X	X	X	

[1] An "X" in this column suggests that in all ISE Privacy Guidelines activities requiring identifying and assessing internal agency privacy policies, the user may be able to leverage a similar activity required by OMB 06-15, which requires each agency's Senior Official for Privacy to conduct a review of privacy policies and processes and take corrective actions wherever deficiencies are found.

[2] An "X" in this column suggests that in all ISE Privacy Guidelines activities requiring identifying and assessing internal agency privacy policies, the user may be able to leverage a similar activity required by OMB 07-16, which requires each agency to review whether policies exist in four areas: (1) general privacy and security policy; (2) incident reporting and handling; (3) external breach notification; and (4) the responsibilities of individuals authorized to access personally identifiable information. OMB 07-16 further requires each agency to draft policies in these areas if none are found and provides guidelines for their scope and terms.

STAGE I								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15[1]**	**OMB M-07-16[2]**	**Comment**
1	2 of 6	Identify sharing (dissemination of terrorism information among ISE participants) laws, Executive Orders, policies, and procedures.	X	—	X	X	X	
1	2 of 6	Identify management (oversight and governance of the above practices and processes) laws, Executive Orders, policies, and procedures.	X	X	—	—	X	
2	3 of 6	**Assess** and identify gaps between existing protections and the protections identified in the ISE Privacy Guidelines.	—	X	—	X	—	
2	3 of 6	Determine and document agency-wide information privacy and civil liberties policies, procedures, guidelines, and practices.	—	—	—	—	—	
2	3 of 6	Agencies should work with affected agency components to determine and document the agency's privacy and civil liberties legal and policy environment for terrorism information sharing.	—	—	—	—	—	
2	3 of 6	Agencies should review what legal authorities are controlling or relevant.	—	—	—	—	—	
2	3 of 6	Agencies should review what information may or may not be collected.	X	—	—	X	X	
2	3 of 6	Agencies should review how information can be collected.	X	—	—	X	X	
2	3 of 6	Agencies should review eligible parties (internal and external) to receive information that is collected.	X	—	—	X	X	
2	3 of 6	Agencies should review their transparency policies.	X	—	X	X	X	
2	3 of 6	Agencies should review their redress policies.	X	—	X	X	X	
2	3 of 6	Agencies should review their accountability, enforcement, and training policies.	X	—	X	X	X	

STAGE I								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15[1]**	**OMB M-07-16[2]**	**Comment**
2	3 of 6	Work with agency components to determine agency-wide information privacy and civil liberties policies, procedures, guidelines, and practices.	—	—	—	—	X	
2	3 of 6	Review whether or not the Fair Information Principles are employed.						
2	3 of 6	Review which records are Privacy Act versus non-Privacy Act records.	X	X	X	—	—	
2	3 of 6	Review "minimum necessary" information sharing policies, procedures, guidelines, practices.	X	—	—	—	X	
2	3 of 6	Review limitations on redisclosure policies, procedures, guidelines, and practices.	X	—	—	—	X	
2	3 of 6	Review any alerts as to the reliability of the information.	X	—	—	—	—	
2	3 of 6	Review policies, procedures, guidelines, and practices around monitored disclosure.	—	—	—	X	X	
2	3 of 6	Review information retention practices.	X	—	—	X	X	
2	3 of 6	Review information security controls.	X	—	X	X	X	
2	3 of 6	Assess how commercial data (information obtained from a commercial source) is collected or stored and used.	—	—	—	—	—	
2	3 of 6	Assess whether commercial data sharing arrangement protections are applied.	—	—	—	—	—	
2	3 of 6	Assess whether commercial data has assurances on reliability applied.	—	—	—	—	—	
2	3 of 6	Assess whether commercial data has sharing alerts applied.	—	—	—	—	—	
2	3 of 6	Assess whether commercial data has verification requirements applied.	—	—	—	—	—	

STAGE I								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15[1]**	**OMB M-07-16[2]**	**Comment**
2	3 of 6	Agencies may find it useful to identify or create a policy manual or comprehensive repository of all privacy and civil liberties policies and procedures necessary for documenting consistency with the ISE Privacy Guidelines.	—	X	—	—	X	
2	4 of 6	Use the "As-Is" state data to compare what is required by the ISE Privacy Guidelines (the "To-Be" state).	—	—	—	X	X	
2	4 of 6	Identify areas where no privacy and civil liberties policy or procedure exists.	—	—	—	—	—	
2	4 of 6	Identify areas where privacy and civil liberties policy or procedures are not adhered to.	—	X	—	—	—	
2	4 of 6	Identify areas where privacy and civil liberties policy or procedures are misunderstood or lack implementation guidance.	—	X	—	—	—	
2	4 of 6	Identify areas where existing privacy and civil liberties policy, procedures, or practices are insufficient to address the ISE Privacy Guidelines requirements.	—	—	—	—	—	
2	4 of 6	Identify areas where training regarding privacy and civil liberties policy and procedures does not sufficiently address the ISE Privacy Guidelines requirements.	—	X	—	—	—	
2	4 of 6	Consider whether the agency seeks and retains only what it is permitted to collect and retain.	X	—	—	—	—	
2	4 of 6	Consider whether data is only collected lawfully.	X	—	—	—	—	
2	4 of 6	Identify interagency rules that impede sharing without protecting privacy, and identify what purpose each restriction is designed to serve.	X	—	—	—	—	
2	4 of 6	Raise issue of impeding interagency rules with the Privacy Guidelines Committee.	—	—	—	—	—	

STAGE I								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15[1]**	**OMB M-07-16[2]**	**Comment**
2	4 of 6	Ensure that information identified within the ISE and shared via ISE processes is used consistent with the provisions of Executive Order 13388, for the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States.	—	—	—	—	—	
3	5 of 6	Ensure that all protected information in the ISE is covered by applicable privacy policies.	—	—	—	—	—	
3	5 of 6	Document that existing laws, Executive Orders, policies, and procedures are in compliance with the ISE Privacy Guidelines.	—	—	—	—	—	
3	5 of 6	Develop new policies to fill any gaps, and bring the agency into compliance with the ISE Privacy Guidelines.	—	—	—	X	X	
3	5 of 6	Agencies must have a written ISE privacy protection policy stating that protected information shall be shared among agencies, organizations, and other persons only as allowed by the agency's information sharing policy and guidelines collected in a manual or held in a central repository.	—	—	—	—	—	
3	5 of 6	Agencies must have protocols and guidelines that define categories of information that may be shared.	—	—	—	—	X	
3	5 of 6	Agencies must have protocols and guidelines that define categories of entities with which data may be shared, with restrictions for each (law enforcement agencies, intelligence agencies, commercial entities, individuals who are the subjects of records, etc.).	X	—	—	—	X	
3	5 of 6	Agencies must have protocols and guidelines that determine information sharing sources (e.g., systems of records/databases).	—	—	—	X	X	

STAGE I								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15[1]**	**OMB M-07-16[2]**	**Comment**
3	5 of 6	Agencies must have protocols and guidelines that determine information sharing methods (e.g., software applications or other media).	—	—	—	—	X	
3	5 of 6	Agencies must have protocols and guidelines that determine how sharing requests may be received.	X	—	—	—	X	
3	5 of 6	Agencies must have protocols and guidelines that determine what processing must be conducted prior to sharing (formatting, redaction, review, etc.).	X	—	—	—	X	
3	5 of 6	Agencies must have protocols and guidelines that determine information sharing protocols (encryption, de-identification/anonymization, documentation, and auditing).	—	—	—	—	X	
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding identity and authorities of information requester/receiver and sender.	X	—	—	—	—	
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding required privacy and civil liberties protections (encryption, limited-use agreements, data retention, notice and consent of data subjects where applicable, minimum necessary data shared).	X	—	—	—	—	
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding required security protections (firewalls, intrusion detection systems, physical security, training and awareness of staff, authorization and authentication, etc.).	X	—	X	—	—	
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding dispute	—	—	—	—	—	

STAGE I								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15[1]**	**OMB M-07-16[2]**	**Comment**
		resolution process.						
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding rights in data, if applicable.	—	—	—	—	—	
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding limitations on redisclosure.	X	—	—	—	—	
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding effects of laws and regulations (including exemptions therefrom).	X	—	—	—	—	
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding disclaimers of warranties/assurances of accuracy.	X	—	—	—	—	
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding monitoring/auditing responsibilities of sender and receiver (methods, frequency, roles and responsibilities, remediation).	—	—	—	—	—	
3	5 of 6	New or existing policies should include an overarching policy for the periodic and careful review of agency and personnel compliance with privacy and civil liberties procedures (such as through an inspection/review process).	—	—	—	X	—	
3	6 of 6	New or existing policies should include an overarching mechanism for promptly reporting noncompliance with all ISE privacy and civil liberties procedures.	—	—	—	—	—	

STAGE I								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15[1]**	**OMB M-07-16[2]**	**Comment**
3	6 of 6	New or existing policies should include an overarching mechanism for responding to incidents of noncompliance, including sanctions for individuals that are negligently or willfully noncompliant.	X	—	—	—	—	
3	6 of 6	New or existing policies should include policies on computer matching and other data-merges, including implications of the Privacy Act.	X	—	—	X	X	
3	6 of 6	New or existing policies should include posting of Systems of Record Notices (SORNs) and other Privacy Act requirements, if applicable.	X	—	—	—	X	
3	6 of 6	New or existing policies should include data accuracy, completeness, and timeliness controls.	X	—	—	—	X	
3	6 of 6	Agencies developing new policies/procedures should address relevant federal laws, regulations, guidelines, interagency agreements or rules, or other agency-specific directives driving each requirement, especially those restricting data sharing.	X	—	—	—	X	
3	6 of 6	Agencies developing new policies/procedures should address the specific mandatory required action or end state.	—	—	—	—	X	
3	6 of 6	Agencies developing new policies/procedures should address any exemptions to each requirement that the agency may invoke or has invoked, if applicable.	—	—	—	—	X	
3	6 of 6	Agencies developing new policies/procedures should address the specific officials and personnel affected by the policies and those responsible for implementation and oversight.	—	—	—	—	X	

STAGE I								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15[1]**	**OMB M-07-16[2]**	**Comment**
3	6 of 6	Agencies developing new policies/procedures should address the particular detailed procedures to be followed by each category of affected staff, including enforcement and assurance responsibilities.	—	—	—	—	X	

STAGE II								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15**	**OMB M-07-16**	**Comments**
1	2 of 5	**Identify** the terrorism information systems, sharing arrangements, and "protected information" that are currently being shared or could be shared in the ISE.	—	—	—	—	—	
1	2 of 5	Agencies will need to identify existing systems and databases that contain terrorism information (personally identifiable information currently shared by law or agency policy, including interagency memoranda of agreement or other sharing arrangements). (Note: If agencies already have a process that covers this step, they do not need to do additional assessments of those systems solely for the purpose of the ISE Privacy Guidelines.)	—	—	—	—	—	
1	2 of 5	Agencies will need to identify existing systems and databases that contain terrorism information that will potentially be shared through the ISE. (Note: If agencies already have a process that covers this step, they do not need to do additional assessments of those systems solely for the purpose of the ISE Privacy Guidelines.)	—	—	—	—	—	
1	2 of 5	Agencies should analyze the Green Pages to ensure that systems of records/databases are appropriately identified as Category I.	—	—	—	—	—	
1	2 of 5	Agencies should identify any information sharing agreements and other arrangements that exist or are planned for Category I systems and databases contained within the Green Pages.	—	—	—	—	—	

STAGE II								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15**	**OMB M-07-16**	**Comments**
1	2 of 5	Agencies should identify their systems of records/databases that are clearly Category I, although not identified in the Green Pages.	—	—	—	—	—	
1	2 of 5	Agencies should identify any information sharing agreements and other arrangements that exist or are planned for Category I systems and databases not contained in the Green Pages.	—	—	—	—	—	
1	2 of 5	Agencies should identify their Category II systems of records/databases that contain a mix of terrorism and nonterrorism information.	—	—	—	—	—	
1	2 of 5	Agencies should identify any information sharing agreements and other arrangements that exist or are planned for Category II systems and databases.	—	—	—	—	—	
1	2 of 5	Agencies should identify their Category III systems of records/databases that contain information that is clearly not terrorism information but that may become subject to ISE sharing as part of a terrorism investigation.	—	—	—	—	—	
1	2 of 5	Agencies should identify any information sharing agreements and other arrangements that exist or are planned for Category III systems and databases.	—	—	—	—	—	
1	2 of 5	For Category II and III systems of records/databases, identify the risk environment around those containing PII terrorism information to determine whether special protections are warranted.	—	—	—	—	—	

STAGE II								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15**	**OMB M-07-16**	**Comments**
1	3 of 5	To identify the risk environment for systems of records/databases, determine whether the system of record/database contains sensitive information that is subject to privacy and civil liberties protections (e.g., personally identifiable information that reveals medical, financial, or religious information).	—	—	X	—	—	
1	3 of 5	To identify the risk environment for systems of records/databases, determine what specific protections each category of information must receive under legal, regulatory, or contractual obligations.	—	—	X	—	—	
1	3 of 5	To identify the risk environment for systems of records/databases, determine what information privacy policies and practices are applied.	—	—	X	—	—	
1	3 of 5	To identify the risk environment, determine whether privacy protection exemptions assigned to the data or system apply if the information is shared within the ISE.	—	—	X	—	—	
1	3 of 5	To identify the risk environment, determine the likelihood that the data will be shared within the ISE.	—	—	X	—	—	
1	3 of 5	To identify the risk environment, determine how each category of information under consideration could be exploited if it were inappropriately disclosed, accessed, or intercepted.	—	—	X	—	—	
1	3 of 5	To identify the risk environment, determine what harms would result to the individual if information were inappropriately disclosed, accessed, or intercepted.	—	—	X	—	—	

STAGE II								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15**	**OMB M-07-16**	**Comments**
1	3 of 5	To identify the risk environment, determine the magnitude of the harms that would result—to the individual, the organization, or to larger interests such as those of the United States—if information were inappropriately disclosed, accessed, or intercepted.	—	—	X	—	—	
1	3 of 5	To identify the risk environment, determine what types of persons would be interested in inappropriately accessing, transmitting, or receiving each type of information, both inside and outside of the agency maintaining it.	—	—	X	—	—	
2	4 of 5	**Assess** and identify the risk to privacy and civil liberties for the terrorism systems identified in Step 1.	—	—	X	—	—	
2	4 of 5	Assess whether the agency's risk assessment criteria was applied to determine whether ISE information shared in the ISE should continue to be shared and, if so, whether special protections are warranted.	—	—	X	—	—	
2	4 of 5	Assess whether the agency's risk assessment criteria (for application to determine whether ISE information under consideration for sharing in the ISE) was applied to determine whether the information should be shared in the ISE and, if so, whether special protections are warranted.	—	—	X	—	—	
2	4 of 5	Agencies must assess their implementation of laws and policies to identified systems.	—	—	—	—	X	

STAGE II								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15**	**OMB M-07-16**	**Comments**
2	4 of 5	To assess application of laws and policies to systems, agencies must assess whether their information privacy and civil liberties marking system that ensures information is handled in accordance with applicable legal requirements is applied to ISE information. (Refer to Notice Mechanisms.)	X	—	—	X	X	
2	4 of 5	To assess application of laws and policies to systems, agencies must assess whether their data quality procedures designed to ensure accuracy, timely correction, and appropriate retention of data are applied to ISE information. (Refer to Data Quality.)	X	—	—	X	X	
2	4 of 5	To assess application of laws and policies to systems, agencies must assess whether their data security procedures designed to safeguard protected information are applied to ISE information. (Refer to Data Security.)	X	—	X	X	X	
2	4 of 5	To assess application of laws and policies to systems, agencies must assess whether their auditing procedures designed to hold personnel accountable, ensure training of staff, and conduct reviews and audits designed to obtain and verify compliance are applied to ISE information. (Refer to Accountability.)	X	X	—	X	X	

STAGE II								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15**	**OMB M-07-16**	**Comments**
2	4 of 5	To assess application of laws and policies to systems, agencies must assess whether their transparency and redress procedures designed to inform the public of agency information and privacy policies and address complaints from persons regarding information under agency control are in place for the ISE. (Refer to Redress.)	X	X	—	X	—	
3	5 of 5	**Protect** by establishing actions that the agency needs to take for "protected information" shared from those identified systems.	X	—	—	—	—	
3	5 of 5	Document agency's protections required for specific systems/information shared in the ISE based on assessment of systems and policy requirements.	—	X	X	X	X	
3	5 of 5	If existing policies or procedures address the required provision, an agency must document that an existing policy or procedure complies with the ISE Privacy Guidelines provision.	—	—	—	—	—	
3	5 of 5	Agencies should put in place a policy that implements required protections for the system.	X	—	—	—	X	
3	5 of 5	Agencies should put in place reporting/notification procedures regarding violations of agency-protection policies, as appropriate, that address reporting, investigating, and responding to such violations.	X	—	—	—	X	
3	5 of 5	Agencies should put in place audit and enforcement mechanisms for the system as required by policy for that system.	X	—	—	—	X	

STAGE II								
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15**	**OMB M-07-16**	**Comments**
3	5 of 5	Agencies should provide training for personnel authorized to share protected information for the system regarding the agency's requirements and policies for collection, use, and disclosure of protected information and as appropriate for reporting violations of agency privacy and civil liberties protection policies.	X	X	—	—	X	
3	5 of 5	Agencies should ensure cooperation with audits and reviews by officials with responsibility for providing oversight with respect to the ISE.	—	—	—	—	—	
3	5 of 5	Agencies should ensure that their designated ISE privacy official receives reports (or copies) regarding alleged errors in protected information that originates from the agency.	—	—	—	—	—	
3	5 of 5	Repeat Stage II as necessary if new or additional systems and sharing arrangements in the ISE are developed and identified.	—	—	—	—	—	